ON THE HAMMING WEIGHT OF REPEATED ROOT CYCLIC AND NEGACYCLIC CODES OVER GALOIS RINGS

SERGIO R. LÓPEZ-PERMOUTH AND STEVE SZABO

Abstract. Repeated root Cyclic and Negacyclic codes over Galois rings have been studied much less than their simple root counterparts. This situation is beginning to change. For example, repeated root codes of length p^s, where p is the characteristic of the alphabet ring, have been studied under some additional hypotheses. In each one of those cases, the ambient space for the codes has turned out to be a chain ring. In this paper, all remaining cases of cyclic and negacyclic codes of length p^s over a Galois ring alphabet are considered. In these cases the ambient space is a local ring with simple socle but not a chain ring. Nonetheless, by reducing the problem to one dealing with uniserial subambients, a method for computing the Hamming distance of these codes is provided.

1. Introduction

Cyclic and negacyclic codes have been studied extensively in many contexts, beginning with their linear versions over finite fields and continuing on to the study of such codes over a finite ring alphabet A. A common element in the study of these codes is that they are precisely the submodules of the free module A^n that correspond to the ideals of a suitable ring R_n which is isomorphic to A^n as an A-module. The ring R_n is either the quotient $\frac{A[x]}{\langle x^n-1\rangle}$ (for the cyclic case) or the quotient ring $\frac{A[x]}{\langle x^n+1\rangle}$ (for the negacyclic case). In either case, we refer to the ring R_n as *the ambient space* or *ambient ring* for the codes. While the literature on cyclic and negacylic codes over chain rings (such as Galois rings) has grown in leaps and bounds (see [4, 10, 11, 17, 18, 21]), in most instances the studies have been focused only on the cases where the characteristic of the alphabet ring is coprime to the code length, the so-called simple root codes. A few of the contributions to the study of the cases where the characteristic of the alphabet ring is not coprime the the code length (repeated root codes) are [1, 2, 5, 9, 16, 19]. In this paper we focus on the repeated root case where the code length is in fact a power of a prime.

Let p be a prime and consider cyclic and negacyclic codes of length p^s over $GR(p^a, m)$. The study of such codes was started in [8] for the negacyclic case when $p = 2$ and $m = 1$. It was shown there that the ambient $\frac{Z_{2^a}[x]}{\langle x^{p^s}+1\rangle}$ is a chain ring. This result was extended to the case when m is arbitrary in [6]. The distances for most of these codes was calculated there. The chain ring structure of the ambient was heavily used to accomplish this goal.

When $a = 1$, the Galois ring $GR(p^a, m)$ is just the Galois field F_{p^m}. Codes over F_{p^m} were consider in [7]. There it was shown that for arbitrary p, the ambient space $\frac{F_{p^m}[x]}{\langle x^{p^s}+1\rangle}$ is a chain ring. Once again the chain structure of the ambient space

was used to compute all the code distances. Then it was shown also in [7] that $\frac{F_{p^m}[x]}{\langle x^{p^s}+1\rangle} \cong \frac{F_{p^m}[x]}{\langle x^{p^s}-1\rangle}$ when p is odd, which allows all the negacyclic results to be carried over to the cyclic code case. It should be noted that over a field of characteristic 2, there is no distinction between cyclic and negacyclic codes since $\frac{F_{2^m}[x]}{\langle x^{p^s}+1\rangle} = \frac{F_{2^m}[x]}{\langle x^{p^s}-1\rangle}$.

In all cases mentioned so far, the codes correspond to principal ideals. This is a consequence of the fact that the code ambients are chain rings. In the remaining cases, which comprise the primary subject of this paper, the code ambients are no longer chain rings and in fact, not even PIRs. There are three remaining cases: negacyclic codes over $GR(p^a, m)$ for odd prime p and $a > 1$ of length p^s; cyclic codes of the same type; cyclic codes over $GR(2^a, m)$ for $a > 1$ of length p^s. In this paper these remaining cases are considered and a method for computing the Hamming distance of any code is provided.

Now, simple root cyclic codes over Z_{p^m} were studied in [4] where a generating set for such codes was formulated and it was also proved that these codes are principal ideals of the ambient ring. An alternative generating set was given for codes over Z_4 in [17]. This result was extended to Z_{p^m} in [10] where they also showed the connection between the two formulations. These results were in turn extended to simple root cyclic codes over Galois rings in [20].

In a series of papers ([18],[14],[15],[13]), the idea of Gröbner basis was extended to principal ideal rings and was used to prove the existence of generating sets with certain desirable properties for cyclic and negacyclic codes over chain rings. Specifically, they showed that given this generating set, the code distance can be determined from one particular element in the generating set. In Section 3, we will use this theory to determine all minimum code distances.

For the most part, the literature preceding ([18],[14],[15],[13]), failed to address specific distance information about cyclic and negacyclic codes. The generating sets given in [4] are based on the factorization of $x^n - 1$. Given a factorization of $x^n - 1$, it is still not simple to compute distances, even in light of the results in [18] mentioned earlier. To use those results in this context, the minimum weights for all principal ideals are needed. Since it was shown that simple root cyclic codes over Galois rings are principal, the results just mentioned bring us no closer to finding distances in the simple root case. In this paper however, we will show that these results can be very useful in determining distances in some multiple root codes where not all of the codes are principal. This method reduces the problem to finding distance information of related codes which are principal.

In Section 2, the necessary background on Galois rings is given together with other results that are needed throughout the paper. Section 3 considers the class of codes in $\frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$ where p is an odd prime and $a > 1$. In this section it is shown that $\frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$ is a local ring with simple socle that is not a chain ring. Then a method for computing Hamming distances is shown. Section 4 examines cyclic codes. When p is odd, there is a one-one correspondence between cyclic and negacylcic codes over $GR(p^a, m)$ of length p^s for odd prime p which is shown. The remainder of the section is devoted to cyclic codes over $GR(2^a, m)$ for $a > 1$ of length p^s. It is shown that $\frac{GR(2^a,m)[x]}{\langle x^{2^s}-1\rangle}$ has a very similar structure to $\frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$ from Section 3. Again a method for computing Hamming distances is shown.

2. Preliminaries

In this paper, the word *ring* means finite commutative ring with identity. The only exception is when we talk about the (infinite) ring $R[x]$ of polynomials with coefficients in the ring R. A *local ring* is a ring with a unique maximal ideal. Given a commutative ring R, the *Jacobson radical* of R, denoted by $J(R)$, is the intersection of all maximal ideals of R and the *socle* of R, denoted by $soc(R)$, is the sum of all minimal ideals of R. A polynomial $f(x) \in R[x]$ is *regular* if it is not a zero divisor. The following is a characterization of regular polynomials in polynomial rings over local rings.

Lemma 2.1 (Theorem XIII.2, [12])**.** *Let R be a finite local commutative ring and $f(x) \in R[x]$ where $f(x) = a_0 + \cdots + a_n x^n$ for $a_i \in R$. The following are equivalent:*

1. *f is a regular polynomial.*
2. *$\langle a_0, \ldots, a_n \rangle = R$.*
3. *a_i is a unit for some $0 \leq i \leq n$.*
4. *$f(x) \pmod p \neq 0$.*

Polynomial rings over local rings admit a division algorithm for certain polynomials.

Lemma 2.2 (Proposition 3.4.4, [3])**.** *Let R be a finite local commutative ring and $f(x), g(x) \in R[x]$ where $g(x)$ is regular. Then there exists $q(x), r(x) \in R[x]$ such that*

$$f(x) = g(x)q(x) + r(x)$$

with $deg(r) < deg(g)$ or $r(x) = 0$.

A *chain ring* is a ring whose ideals are linearly ordered by inclusion. The following characterization of chain rings is well-known:

Lemma 2.3. *Let R be a finite commutative ring. The following are equivalent:*

1. *R is a chain ring.*
2. *R is a local principal ideal ring.*
3. *R is a local ring with maximal ideal that is principal.*

Galois rings constitute a very important family of finite chain rings. They can be defined as follows: Let $f(x) \in Z_{p^a}[x]$ be a basic irreducible polynomial (a *basic irreducible* polynomial in $Z_{p^m}[x]$ is an irreducible polynomial in $Z_{p^a}[x]$ whose reduction modulo p is irreducible in $Z_p[x]$) and $m = deg(f)$. Then the Galois ring $GR(p^a, m) = \frac{Z_{p^a}[x]}{\langle f(x) \rangle}$. It is well-known that different choices of m and a yield non-isomorphic Galois rings while, on the other hand, distinct choices of $f(x)$ with the same degree m yield the same Galois ring up to isomorphism. We now list a few pertinent details about these rings. For a more detailed account of the theory of Galois rings including proofs of the results we mention here, see [12] or [20].

Every Galois ring $R = GR(p^a, m)$ contains a $(p^m - 1)^{th}$ primitive root of unity ζ. Every $r \in R$ has a p-adic expansion $r = \zeta_0 + \zeta_1 p + \cdots + \zeta_{a-1} p^{a-1}$ where $\zeta_i \in \{0, 1, \zeta, \zeta^2, \ldots, \zeta^{p^m - 2}\}$, the Teichmüller set $\mathcal{T}_m$ of R.

Given a polynomial $f(x)$ in any polynomial ring $R[x]$, f can be viewed in the form $f(x) = \sum_{i=0}^{k} a_i (x+1)^i$ where $a_i \in R$. So, for $f \in GR(p^a, m)[x]$, $f(x) = \sum_{i=0}^{k} \sum_{j=0}^{a} \zeta_{ij} p^j (x+1)^i$ where $\zeta_{ij} \in \{0, 1, \zeta, \zeta^2, \ldots, \zeta^{p^m - 2}\}$.

The next two Lemmas are results on negacyclic code ambients over Galois rings which will be needed in the proceeding sections. Defining multiplication of $r \in \frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$ by $m \in \frac{GR(p,m)[x]}{\langle x^{p^s}+1\rangle}$ as multiplication in $\frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$ mod p, $\frac{GR(p,m)[x]}{\langle x^{p^s}+1\rangle}$ can be made into an $\frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$-module. In light of this, the following lemma is easy to see.

Lemma 2.4. *For any prime p, the $\frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$-modules $p^{a-1}\frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$ and $\frac{GR(p,m)[x]}{\langle x^{p^s}+1\rangle}$ are isomorphic.*

Lemma 2.5 ([7], Proposition 3.2)**.** *For any prime p, the ambient ring $\frac{GR(p,m)[x]}{\langle x^{p^s}+1\rangle}$ is a chain ring with exactly the following deals,*

$$\frac{GR(p,m)[x]}{\langle x^{p^s}+1\rangle} = \langle (x+1)^0\rangle \supsetneq \cdots \supsetneq \langle (x+1)^{p^s}\rangle = 0.$$

In [14] an algorithm was given to find a Gröbner basis for ideals of a polynomial ring over a PIR. Later in [18], it is shown that any ideal of a residue ring of a polynomial ring over a chain ring has a Gröbner basis with certain additional properties. Since for any prime p, $GR(p^a,m)$ is a chain ring, ideals of $\frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$ will have such a Gröbner basis. The following Lemma is a restatement of that result.

Lemma 2.6 (adapted from Theorem 4.1 in [18])**.** *For any prime p, given an ideal $I \lhd \frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$, for $i \in \{0,\ldots,r\}$ there exist $j_i \in Z$ and $f_i \in \frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$ where $0 \leq r \leq a-1$ such that*

$$I = \langle p^{j_0}f_0, \ldots, p^{j_r}f_r\rangle$$

and

1. $0 \leq j_0 < \cdots < j_r \leq a-1$
2. *f_i monic for $i = 0,\ldots,r$,*
3. $p^s > deg(f_0) > \cdots > deg(f_r)$,
4. $p^{j_{i+1}}f_i \in \langle p^{j_{i+1}}f_{i+1}, \ldots, p^{j_r}f_r\rangle$
5. $p^{j_0}(x^{p^s}+1) \in \langle p^{j_0}f_0, \ldots, p^{j_r}f_r\rangle$ *in $GR(p^a,m)[x]$.*

One can show further that the set of generators in Lemma 2.6 is a strong Gröbner basis in the sense of [18]. While interesting, this fact will not be used here.

Lemma 2.7. *Let p be a prime. Let $k \leq \frac{p^n}{2}$ and l be the largest integer s.t. $p^l \mid k$. Then $p^{n-l} \mid \binom{p^n}{k}$.*

Proof. For $k \leq p$, the result holds. Now we proceed in 3 cases. First assume there is an $l > 0$ s.t. $p^l \mid k-1$ and it is the largest such integer. Then $p^{n-l} \mid \binom{p^n}{k-1}$. Since $p^l \mid k-1$, $p \nmid k$ and $p^l \mid p^n - k + 1$. So, $p^l \mid \frac{p^n-k+1}{k}$. Hence, $p^{n-l+l} \mid \binom{p^n}{k-1}\frac{p^n-k+1}{k} = \binom{p^n}{k}$. Now, assume $p \nmid k-1$ and $p \nmid k$. Then $p \nmid p^n - k + 1$. So, for any l s.t. $p^l \mid \binom{p^n}{k-1}$, $p^l \mid \binom{p^n}{k}$. Noting the previous case, $p^n \mid \binom{p^n}{k}$. Now, assume there is an $l > 0$ s.t. $p^l \mid k$ and it is the largest such integer. Then $p \nmid k-1$ and so $p \nmid p^n - k + 1$. Again noting the previous cases, $p^{n-l} \mid \binom{p^n}{k}$ □

3. Negacyclic codes in $\frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$ for odd prime p

As mentioned earlier, all ambient rings previously studied in the literature are chain rings. They are $\frac{GR(2^a,m)[x]}{\langle x^{2^s}+1\rangle}$, $\frac{GR(p,m)[x]}{\langle x^{p^s}+1\rangle}$ and $\frac{GR(p,m)[x]}{\langle x^{p^s}-1\rangle}$ for $a, m, p, s \in Z$ where $a \geq 1$, $m \geq 1$, p is prime and $s \geq 0$. In the following sections the remaining cases will be studied. In these remaining cases, the ambient spaces are not chain rings. We will show, however, that they are local rings with simple socle.

In this section, the structure of $\frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$ where p is an odd prime and $a > 1$ is studied so that in the following section the structure details can be used to find Hamming distance of all codes. Since $s = 0$ is the trivial case also assume $s > 0$.

We start by showing that $x + 1$ is nilpotent. The calculation of its exact nilpotency is saved for Corollary 3.7.

Proposition 3.1. *In $\frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$, $(x + 1)$ is nilpotent.*

Proof.

$$\begin{aligned}(x+1)^{p^s} &= x^{p^s} + \tbinom{p^s}{p^s-1}x^{p^s-1} + \cdots + \tbinom{p^s}{1}x + 1 \\ &= x^{p^s} + 1 + p\alpha(x) \\ &= p\alpha(x)\end{aligned}$$

where $\alpha(x) \in \frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$. Then $(x + 1)^{p^s a} = p^a(\alpha(x))^a = 0$. □

Proposition 3.2. *The ambient ring $\frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$ is local with radical $J\left(\frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}\right) = \langle p, x + 1\rangle$.*

Proof. Let I be the set of non-invertible elements. Let $f \in \langle p, x+1\rangle$. By Proposition 3.1 $(x + 1)$ is nilpotent. Since p is also, f is nilpotent and hence not invertible. So, $\langle p, x + 1\rangle \subset I$. Now, let $f \in I$. We can write $f(x) = \sum_{i=0}^{k} a_i(x + 1)^i$ where $a_i \in GR(p^a, m)$. So, f is invertible if and only if a_0 is invertible. The p-adic expansion $a_0 = \sum_{i=0}^{a-1} b_i p^i$ where $b_i \in \{0, 1, \zeta, \zeta^2, \ldots, \zeta^{p^{m-2}}\}$ assures that a_0 is invertible if and only if $b_0 \neq 0$. The assumption that f not invertible implies therefore, that $p \mid a_0$ and this shows that $f \in \langle p, x + 1\rangle$. So, $I \subset \langle p, x + 1\rangle$. Since I contains all invertible elements, it is the unique maximal ideal and therefore, $\frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$ is local. □

Proposition 3.3. *The socle $soc\left(\frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}\right)$ of $\frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$ is the simple module $\langle p^{a-1}(x + 1)^{(p^s-1)}\rangle$.*

Proof. Using Lemma 2.5, it can be shown that $\langle p^{a-1}(x+1)^{(p^s-1)}\rangle \subset soc\left(\frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}\right)$. Let $a(x) \in soc\left(\frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}\right)$. Since $J(\frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}) = \langle p, x + 1\rangle$, $pa(x) = 0$ and $(x+1)a(x) = 0$ so $a(x) \in \langle p^{a-1}(x + 1)^{p^s-1}\rangle$. Hence, $soc\left(\frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}\right) = \langle p^{a-1}(x + 1)^{(p^s-1)}\rangle$.

By Lemmas 2.4 and 2.5, it is clear that $soc\left(\frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}\right)$ is simple. □

Proposition 3.4. *In the ambient ring $\frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$*

(1) $p \notin \langle x + 1\rangle$
(2) $x + 1 \notin \langle p\rangle$

(3) $\frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$ *is not a chain ring*
(4) $\langle p, x+1\rangle$ *is not a principal ideal*

Proof. Assume $p \in \langle x+1\rangle$. So, $p = (x+1)f(x) + (x^{p^s}+1)g(x)$ in $GR(p^a,m)[x]$. When $x=-1$, $p=0$ which is a contradiction in this case since $a \neq 1$. Hence, $p \notin \langle x+1\rangle$.

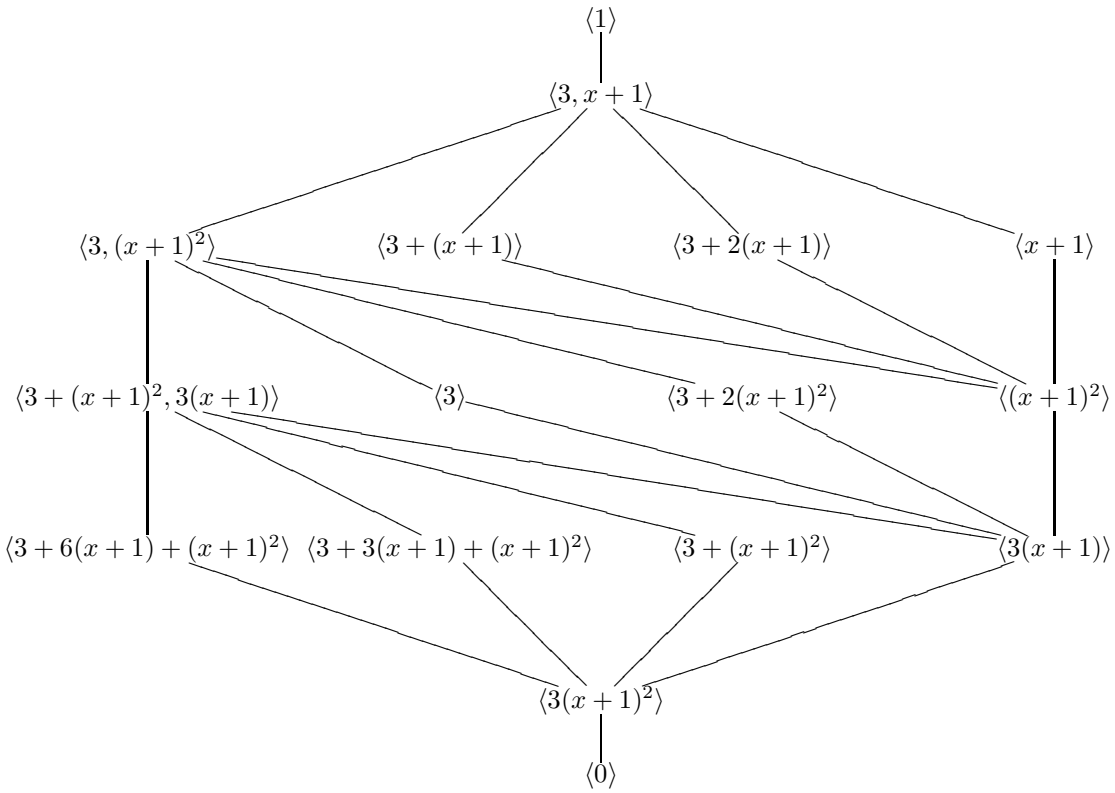
Now assume $x+1 \in \langle p\rangle$. Then $x+1 = pf(x) + (x^{p^s}+1)g(x)$. Now, comparing coefficients, $1 = pf_0 + g_0$ which implies $1 \equiv g_0$ modulo p. Also, $0 = pf_{p^s} + g_0 + g_{p^s}$ which implies $g_0 \equiv -g_{p^s}$ modulo p. In general, $0 = pf_{kp^s} + g_{(k-1)p^s} + g_{kp^s}$ for $k \geq 1$. So, $g_{kp^s} \neq 0$ for $k \geq 0$ which is a contradiction since g is a polynomial. Hence, $x+1 \notin \langle p\rangle$.

Finally, since $0 \neq \langle p\rangle \subsetneq \langle x+1\rangle$ and $0 \neq \langle x+1\rangle \subsetneq \langle p\rangle$, $\frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$ is not a chain ring. Since any local ring with principal maximal ideal is a chain ring by Lemma 2.3, $\frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$ cannot have principal maximal ideal. Hence, $\langle p, x+1\rangle$ is 2-generated. □

Theorem 3.5. *The ambient ring* $\frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$ *is a finite local ring with simple socle but not a chain ring.*

Proof. Result of Propositions 3.2, 3.3 and 3.4. □

Example 1. *To illustrate Theorem 3.5, we provide the following figure. It shows the ideal lattice of* $\frac{Z_{3^2}[x]}{\langle x^3+1\rangle}$. *Notice that the radical is* $\langle 3, x+1\rangle$ *and the socle is* $\langle 3(x+1)^2\rangle$. *More importantly, we see that the ring is not a chain ring.*



Now we are ready to develop our main structural Lemma.

Lemma 3.6. *In* $\frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$ *for* $t \geq 0$,

$$(x+1)^{p^s+t(p-1)p^{s-1}} = p^{t+1}b_t(x)(x+1)^{p^{s-1}} + a_t(x)$$

where $b_t(x)$ *is invertible and* $p^{t+2}|a_t(x)$.

Proof. We proceed by induction on t. For $t = 0$,

$$\begin{aligned} 0 = x^{p^s}+1 &= ((x+1)-1)^{p^s}+1 \\ &= (x+1)^{p^s} - \tbinom{p^s}{p^s-1}(x+1)^{p^s-1} + \tbinom{p^s}{p^s-2}(x+1)^{p^s-2} - \cdots + \tbinom{p^s}{1}(x+1) \end{aligned}$$

By Lemma 2.7

$$\begin{aligned} (x+1)^{p^s} &= \tbinom{p^s}{p^s-1}(x+1)^{p^s-1} - \tbinom{p^s}{p^s-2}(x+1)^{p^s-2} + \cdots - \tbinom{p^s}{1}(x+1) \\ &= \tbinom{p^s}{(p-1)p^{s-1}}(x+1)^{(p-1)p^{s-1}} + \cdots - \tbinom{p^s}{p^{s-1}}(x+1)^{p^{s-1}} + a_0(x) \\ &= pb_0(x)(x+1)^{p^{s-1}} + a_0(x) \end{aligned}$$

for some $a_0(x)$ s.t. $p^2|a_0(x)$ and $b_0(x)$ invertible.

Now assume the result holds for $t-1$. So there exists some $a_{t-1}(x)$ s.t. $p^{t+1}|a_{t-1}(x)$ and $b_{t-1}(x)$ invertible where $(x+1)^{p^s+(t-1)(p-1)p^{s-1}} = p^t b_{t-1}(x)(x+1)^{p^{s-1}} + a_{t-1}(x)$. So

$$\begin{aligned} (x+1)^{p^s+t(p-1)p^{s-1}} &= (x+1)^{p^s+(t-1)(p-1)p^{s-1}}(x+1)^{(p-1)p^{s-1}} \\ &= \left[p^t b_{t-1}(x)(x+1)^{p^{s-1}} + a_{t-1}(x)\right](x+1)^{(p-1)p^{s-1}} \\ &= p^t b_{t-1}(x)(x+1)^{p^s} + a_{t-1}(x)(x+1)^{(p-1)p^{s-1}} \\ &= p^t b_{t-1}(x)\left[pb_0(x)(x+1)^{p^{s-1}} + a_0(x)\right] + a_{t-1}(x)(x+1)^{(p-1)p^{s-1}} \\ &= p^{t+1}b_{t-1}(x)b_0(x)(x+1)^{p^{s-1}} + p^t b_{t-1}(x)a_0(x) + a_{t-1}(x)(x+1)^{(p-1)p^{s-1}} \\ &= p^{t+1}b_{t-1}(x)\left[b_0(x) + \tfrac{a_{t-1}(x)}{p^{t+1}}(x+1)^{(p-2)p^{s-1}}\right](x+1)^{p^{s-1}} + p^t b_{t-1}(x)a_0(x) \\ &= p^{t+1}b_t(x)(x+1)^{p^{s-1}} + a_t(x) \end{aligned}$$

□

Corollary 3.7. *In* $\frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$, *the nilpotency of* $x+1$ *is* $p^s a - p^{s-1}(a-1)$.

Proof. By Lemma 3.6,

$$(x+1)^{p^s+(a-2)(p-1)p^{s-1}} = p^{a-1}b(x)(x+1)^{p^{s-1}} + a(x)$$

for some $b(x)$ is invertible and $a(x)$ s.t. $p^a|a(x)$. So, $a(x) = 0$ and

$$(x+1)^{p^s+(a-2)(p-1)p^{s-1}} = p^{a-1}b(x)(x+1)^{p^{s-1}}.$$

So,

$$(x+1)^{p^s+(a-2)(p-1)p^{s-1}}(x+1)^{(p-1)p^{s-1}-1} = p^{a-1}b(x)(x+1)^{p^s-1}$$

meaning

$$(x+1)^{p^s+(a-1)(p-1)p^{s-1}-1} = p^{a-1}b(x)(x+1)^{p^s-1} \neq 0.$$

Finally,

$$(x+1)^{p^s+(a-1)(p-1)p^{s-1}} = p^{a-1}b(x)(x+1)^{p^s} = 0$$

Hence the nilpotency of $x+1$ is $p^s + (a-1)(p-1)p^{s-1} = p^s a - p^{s-1}(a-1)$. □

So far we have seen that $\frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$ is not a chain ring and not even a PIR. Although a description of a generating set for ideals would be most desirable, we will settle for a bound on the number of generators. We provide two proofs of this result. The first one has a more theoretical flavor as it uses results from [12] on polynomial rings over local rings. The second one aims at establishing a simple algorithm for producing such a generating set.

Lemma 3.8. *In the ambient ring $\frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$, any ideal is generated by a or fewer elements.*

Proof #1. Let $I = \langle f_0, f_1, \ldots, f_n\rangle \subset GR(p^a,m)[x]$ where $f_i \in GR(p^a,m)[x]$ and $deg(f_i) < p^s$. There exists a regular polynomial $g_i \in GR(p^a,m)[x]$ where $f_i = p^{k_i}g_i$. Consider $f_a \neq f_b$ where $deg(f_a) \geq deg(f_b)$. If $k_a = k_b$, by using Lemma 2.2 on g_a and g_b, $f_a \in \langle f_b, r\rangle$ where $r(x) = 0$ or $deg(r) < deg(f_b)$. So, at this point $I = \langle f_0, f_1, \ldots, f_{a-1}, r, f_{a+1}, \ldots, f_n\rangle$. If $p^{k_b+1} \nmid r(x)$, we can continue this process and replace f_j and then r etc. until the remainder is divisible by p^{k_j+1}. It is clear then using this process that it will produce a generating set $I = \langle g_0, p^1g_1, \ldots, p^{a-1}g_{a-1}\rangle$ where either each $g_i = 0$ or is a regular polynomial. □

For the second proof, a canonical form for the description of polynomials is needed. It was shown earlier that any $f \in \frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$ can be written as

$$f(x) = \sum_{i=0}^{p^s-1}\sum_{j=0}^{a-1} \zeta_{ij}p^j(x+1)^i$$

where $\zeta_{ij} \in \{0, 1, \zeta, \zeta^2, \ldots, \zeta^{p^m-2}\} = \mathcal{T}_m$. Now, we will show there is a useful form which we call the canonical form. First, we can write

$$f(x) = \beta_0p^0(x+1)^{i_0}\alpha_0(x) + \beta_1p^1(x+1)^{i_1}\alpha_1(x) + \cdots + \beta_{a-1}p^{a-1}(x+1)^{i_{a-1}}\alpha_{a-1}(x)$$

where $\beta_k \in \mathcal{T}_m$ and $\alpha_k(x) \in \frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$ is invertible. Assume for a moment that $i_{k_1} \leq i_{k_2}$ and $\beta_{k_1} \neq 0 \neq \beta_{k_2}$ for some $k_1 \neq k_2$. Then

$$\beta_{k_1}p^{k_1}(x+1)^{i_{k_1}}\alpha_{k_1} + \beta_{k_2}p^{k_2}(x+1)^{i_{k_2}}\alpha_{k_2} = \beta_{k_1}p^{k_1}(x+1)^{i_{k_1}}(\alpha_{k_1} + \frac{\beta_{k_2}}{\beta_{k_1}}p^{k_2-k_1}(x+1)^{i_{k_2}-i_{k_2}}\alpha_{k_2}).$$

Since $\alpha_{k_1} + \frac{\beta_{k_2}}{\beta_{k_1}}p^{k_2-k_1}(x+1)^{i_{k_2}-i_{k_2}}\alpha_{k_2}$ is invertible, wlog we can assume $i_0 > i_1 > \cdots > i_{a-1}$. We now use this canonical form in the following proof.

Proof #2. Let $I = \langle g_0, g_1, \ldots, g_n\rangle$ where $g_j \in \frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$. If $n \leq a-1$ we are done so assume $n \geq a$. Let $f_j = g_j$. Viewing the f_j in canonical form, write

$$f_j(x) = \beta_{j0}p^0(x+1)^{i_{j0}}\alpha_{j0}(x) + \cdots + \beta_{j(a-1)}p^{a-1}(x+1)^{i_{j(a-1)}}\alpha_{j(a-1)}(x).$$

If $\beta_{j0} \neq 0$ for some j, we reorder the f_j so that for all j where $\beta_{j0} \neq 0$, $i_{00} \leq i_{j0}$. Then, let

$$f'_j(x) = f_j - \beta_{00}^{-1}\alpha_{00}^{-1}f_0(x)\beta_{j0}\alpha_{j0}(x)(x+1)^{i_{j0}-i_{00}}.$$

If $\beta_{j0} = 0$ for all j, let $f'_j(x) = f_j$. In either case, $f'_j \in I$ and $f_j \in \langle f_0, f'_1, \ldots, f'_n\rangle$. Note that $\beta'_{j0} = 0$ for $j \geq 1$. To avoid unnecessary complication with the notation at this point we let $f_j = f'_j$. Next we do the same process but we leave f_0 alone. If $\beta_{j1} \neq 0$ for some $j \geq 1$, we reorder the f_j so that for all $j \geq 1$ where $\beta_{j1} \neq 0$, $i_{11} \leq i_{j1}$. Then, let $f'_j(x) = f_j - \beta_{11}^{-1}\alpha_{11}{}^{-1}f_1(x)\beta_{j1}\alpha_{j1}(x)(x+1)^{i_{j1}-i_{11}}$. If $\beta_{j1} = 0$ for all $j \geq 1$, let $f'_j(x) = f_j$. In either case, $f'_j \in \langle f_0, f_1, \ldots, f_n\rangle$ and

$f_j \in \langle f_0, f_1, f_2' \ldots, f_n' \rangle$. Note that $\beta_{j1}' = 0$ for $j \geq 2$. Continuing this process $a-1$ steps, we end up with

$$\begin{aligned}
f_0(x) &= \beta_{00}(x+1)^{i_{00}}\alpha_{00}(x) + \beta_{01}(x+1)^{i_{01}}\alpha_{01}(x) + \cdots + \beta_{0(a-1)}(x+1)^{i_{0(a-1)}}\alpha_{0(a-1)}(x) \\
f_1(x) &= \beta_{11}(x+1)^{i_{11}}\alpha_{11}(x) + \beta_{12}(x+1)^{i_{12}}\alpha_{12}(x) + \cdots + \beta_{1(a-1)}(x+1)^{i_{1(a-1)}}\alpha_{1(a-1)}(x) \\
&\vdots \\
f_{a-2}(x) &= \beta_{(a-2)(a-2)}(x+1)^{i_{(a-2)(a-2)}}\alpha_{(a-2)(a-2)}(x) + \beta_{(a-2)(a-1)}(x+1)^{i_{(a-2)(a-1)}}\alpha_{(a-2)(a-1)}(x) \\
f_{a-1}(x) &= \beta_{(a-1)(a-1)}(x+1)^{i_{(a-1)(a-1)}}\alpha_{(a-1)(a-1)}(x) \\
f_a(x) &= 0 \\
f_{a+1}(x) &= 0 \\
&\vdots \\
f_n(x) &= 0
\end{aligned}$$

Finally, we see $g_j \in \langle f_0, f_1, f_2, \ldots, f_{a-1} \rangle = I$. □

To illustrate the previous algorithmic proof, we provide the following example.

Example 2. *Let* $f_1, f_2, f_3 \in \frac{Z_9[x]}{x^{27}+1}$ *s.t.*

$$\begin{aligned}
f_1(x) &= (x+1) - 3 \\
f_2(x) &= (x+1)^2 + 3(x+1) \\
f_3(x) &= (x+1)^3 + 3(x+1)
\end{aligned}$$

After applying the first step in the algorithm in the above proof we have

$$\begin{aligned}
f_2'(x) &= f_2(x) - f_1(x)(x+1) = 6(x+1) \\
f_3'(x) &= f_2(x) - f_1(x)(x+1)^3 = 3(x+1)[1 + (x+1)]
\end{aligned}$$

Then one final step gives

$$f_3''(x) = f_3'(x) + f_2'(x)[1 + (x+1)] = 0$$

So, $\langle f_1, f_2, f_3 \rangle = \langle f_1, f_2' \rangle$.

We conclude this section by providing a method for finding the Hamming distances of codes in $\frac{GR(p^a,m)[x]}{\langle x^{p^s}+1 \rangle}$ where p is an odd prime and $a > 1$ is provided. We use the canonical definition of Hamming weight for polynomial based codes i.e. given $\bar{c}(x) \in \frac{GR(p^a,m)[x]}{\langle x^{p^s}+1 \rangle}$ where we consider $c(x)$ as the polynomial representative of degree less than p^s in the coset $\bar{c}(x) = c(x) + \langle x^{p^s} + 1 \rangle$, the Hamming weight of $\bar{c}(x)$, $w(\bar{c}(x))$, is the number of non-zero coefficients of $c(x)$. The minimum distance d is then defined in the usual way.

Remark 1. *It should be clear that the isomorphism in Lemma 2.4 is an isometry when the Hamming weight in* $\frac{GR(p,m)[x]}{\langle x^{p^s}+1 \rangle}$ *is defined similarly to the weight in* $\frac{GR(p^a,m)[x]}{\langle x^{p^s}+1 \rangle}$.

Theorem 4.11 of [7] provides the distances for any code in $\frac{GR(p,m)[x]}{\langle x^{p^s}+1 \rangle}$, which we include here.

Lemma 3.9 (Theorems 4.11, [7]). *In* $\frac{GR(p,m)[x]}{\langle x^{p^s}+1\rangle}$, *for* $0 \leq i \leq p^s$

$$d(\langle (x+1)^i \rangle) = \begin{cases} 1 & \text{if } i = 0, \\ \beta + 2 & \text{if } \beta p^{s-1} + 1 \leq i \leq (\beta+1)p^{s-1} \text{ where } 0 \leq \beta \leq p-2, \\ (t+1)p^k & \text{if } p^s - p^{s-k} + (t-1)p^{s-k-1} + 1 \leq i \leq p^s - p^{s-k} + tp^{s-k-1}, \\ & \text{where } 1 \leq t \leq p-1 \text{ and } 1 \leq k \leq s-1, \\ 0 & \text{if } i = p^s, \end{cases}$$

Using one additional result from [18] the distances of all codes in $\frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$ can be found. Moreover, Lemma 2.6 is algorithm based, so using all these results, an algorithm exists for finding the distances of these codes.

Lemma 3.10 (adapted from Theorem 6.1 in [18]). *Given the set a set a generators for a code* $I \lhd \frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$ *as in Lemma 2.6,* $d(I) = d(\langle p^{a-1} f_r \rangle)$.

Remark 2. *Given Remark 1 and Lemmas 3.9 and 3.10, the distance of any code in* $\frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$ *can be determined. Let* $I \lhd \frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$. *We can find* $f_1, \ldots, f_r \in \frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$ *such that* $I = \langle p^{j_0} f_0, \ldots, p^{j_r} f_r \rangle$ *where this set satisfies the properties of Lemma 2.6. Then Lemma 3.10 implies that* $d(I) = d(\langle p^{a-1} f_r \rangle)$. *Next we view* f_r *in canonical form. Write*

$$f(x) = \beta_0 (x+1)^{i_0} \alpha_0(x) + \beta_1 p^1 (x+1)^{i_1} \alpha_1(x) + \cdots + \beta_{a-1} p^{a-1} (x+1)^{i_{a-1}} \alpha_{a-1}(x)$$

where $\beta_k \in \mathcal{T}_m$ *and* $\alpha_k(x) \in \frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle}$ *is invertible. Note since* f_r *is monic,* $\beta_0 \neq 0$. *So,* $p^{a-1} f_r = p^{a-1} \beta_0 (x+1)^{i_0} \alpha_0(x)$. *Since* β_0 *and* $\alpha_0(x)$ *are units,* $d(I) = d(\langle p^{a-1} f_r \rangle) = d(\langle p^{a-1}(x+1)^{i_0} \rangle)$. *In light of Remark 1, the distance* $d(\langle p^{a-1}(x+1)^{i_0} \rangle)$ *can be found using Lemma 3.9.*

4. Cyclic codes in $\frac{GR(p^a,m)[x]}{\langle x^{p^s}-1\rangle}$ for arbitrary prime p

Let us first consider the case when p is an odd prime. It is easy to see, arguing as in Proposition 5.1 in [8], that $\frac{GR(p^a,m)[x]}{\langle x^{p^s}+1\rangle} \cong \frac{GR(p^a,m)[x]}{\langle x^{p^s}-1\rangle}$ by sending x to $-x$. Hence, all the results can in Section 3 translate easily into results about cyclic codes. Let us therefore focus solely on the case when $p = 2$ for the remainder of this section.

Remember that in [6], it was shown that $\frac{GR(2^a,m)[x]}{\langle x^{2^s}+1\rangle}$ is a chain ring. They also computed the Hamming distance for most of the codes. Let us now consider the cyclic case i.e. the code ambient $\frac{GR(2^a,m)[x]}{\langle x^{2^s}-1\rangle}$. It turns out that when $a > 1$, this is not a chain ring but the structure is very similar to the ring considered in Section 3. In this section assume $a > 1$ and as before $s > 0$ since this produces the trivial case. Most of the proofs here are very similar to their analogs in Section 3. We include only the proofs that need fundamental modification.

Proposition 4.1. *In* $\frac{GR(2^a,m)[x]}{\langle x^{2^s}-1\rangle}$, $(x+1)$ *is nilpotent.*

Proof.

$$\begin{aligned} (x+1)^{2^s} &= x^{2^s} + \tbinom{2^s}{2^s-1} x^{2^s-1} + \cdots + \tbinom{2^s}{1} x + 1 - 1 + 1 \\ &= x^{2^s} - 1 + 2\alpha(x) \\ &= 2\alpha(x) \end{aligned}$$

where $\alpha(x) \in \frac{GR(2^a,m)[x]}{\langle x^{2^s}-1\rangle}$. Then $(x+1)^{2^s a} = 2^a (\alpha(x))^a = 0$. □

The following propositions can be obtained from the parallel results in Section 3 by replacing p with 2 and $x^{p^s}+1$ with $x^{2^s}-1$ and using Proposition 4.1 in lieu of Proposition 3.1 when needed.

Proposition 4.2. *The ambient ring* $\frac{GR(2^a,m)[x]}{\langle x^{2^s}-1\rangle}$ *is local with radical* $J\left(\frac{GR(2^a,m)[x]}{\langle x^{2^s}-1\rangle}\right) = \langle 2, x+1\rangle$.

Proposition 4.3. *The socle* $soc\left(\frac{GR(2^a,m)[x]}{\langle x^{2^s}-1\rangle}\right)$ *of* $\frac{GR(2^a,m)[x]}{\langle x^{2^s}-1\rangle}$ *is the simple module* $\langle 2^{a-1}(x+1)^{(2^s-1)}\rangle$.

Proposition 4.4. *In* $\frac{GR(2^a,m)[x]}{\langle x^{2^s}-1\rangle}$

(1) $2 \notin \langle x+1\rangle$
(2) $x+1 \notin \langle 2\rangle$
(3) $\frac{GR(2^a,m)[x]}{\langle x^{2^s}-1\rangle}$ *is not a chain ring*
(4) $\langle 2, x+1\rangle$ *is not a principal ideal*

Theorem 4.5. *The ambient ring* $\frac{GR(2^a,m)[x]}{\langle x^{2^s}-1\rangle}$ *is a finite local ring with simple socle but not a chain ring.*

Proof. Result of Propositions 4.2, 4.3 and 4.4. □

The following Lemma is similar to Lemma 3.6 with a subtle difference in the divisor of $a_t(x)$ which is used in the last line of the proof.

Lemma 4.6. *In* $\frac{GR(2^a,m)[x]}{\langle x^{2^s}-1\rangle}$ *for* $t \geq 0$,

$$(x+1)^{2^s+t2^{s-1}} = 2^{t+1}b_t(x)(x+1)^{2^{s-1}} + a_t(x)$$

where $b_t(x)$ *is invertible and* $2^{t+2}(x+1)|a_t(x)$.

Proof. We proceed by induction on t. For $t=0$,

$$\begin{aligned} 0 = x^{2^s}-1 &= ((x+1)-1)^{2^s}-1 \\ &= (x+1)^{2^s} - \tbinom{2^s}{2^s-1}(x+1)^{2^s-1} + \tbinom{2^s}{2^s-2}(x+1)^{2^s-2} - \cdots - \tbinom{2^s}{1}(x+1) \end{aligned}$$

By Lemma 2.7

$$\begin{aligned} (x+1)^{2^s} &= \tbinom{2^s}{2^s-1}(x+1)^{2^s-1} - \tbinom{2^s}{2^s-2}(x+1)^{2^s-2} + \cdots + \tbinom{2^s}{1}(x+1) \\ &= \tbinom{2^s}{2^{s-1}}(x+1)^{2^{s-1}} + a_0(x) \\ &= 2b_0(x)(x+1)^{2^{s-1}} + a_0(x) \end{aligned}$$

for some $a_0(x)$ s.t. $2^2(x+1)|a_0(x)$ and $b_0(x) = \frac{\binom{2^s}{2^{s-1}}}{2}$ which is invertible.

Now assume the result holds for $t-1$. So there exists some $a_{t-1}(x)$ s.t. $2^{t+1}(x+1)|a_{t-1}(x)$ and $b_{t-1}(x)$ invertible where $(x+1)^{2^s+(t-1)2^{s-1}} = 2^t b_{t-1}(x)(x+1)^{2^{s-1}} +$

$a_{t-1}(x)$. So

$$\begin{aligned}(x+1)^{2^s+t2^{s-1}} &= (x+1)^{2^s+(t-1)2^{s-1}}(x+1)^{2^{s-1}}\\ &= \left[2^t b_{t-1}(x)(x+1)^{2^{s-1}} + a_{t-1}(x)\right](x+1)^{2^{s-1}}\\ &= 2^t b_{t-1}(x)(x+1)^{2^s} + a_{t-1}(x)(x+1)^{2^{s-1}}\\ &= 2^t b_{t-1}(x)\left[2b_0(x)(x+1)^{2^{s-1}} + a_0(x)\right] + a_{t-1}(x)(x+1)^{2^{s-1}}\\ &= 2^{t+1} b_{t-1}(x)b_0(x)(x+1)^{2^{s-1}} + 2^t b_{t-1}(x)a_0(x) + a_{t-1}(x)(x+1)^{2^{s-1}}\\ &= 2^{t+1} b_{t-1}(x)\left[b_0(x) + \tfrac{a_{t-1}(x)}{2^{t+1}}\right](x+1)^{2^{s-1}} + 2^t b_{t-1}(x)a_0(x)\\ &= 2^{t+1} b_t(x)(x+1)^{2^{s-1}} + a_t(x)\end{aligned}$$

where $2^{t+2}(x+1)|a_t(x)$ and $b_t(x)$ invertible. □

Corollary 4.7. *In* $\frac{GR(2^a,m)[x]}{\langle x^{2^s}-1\rangle}$*, the nilpotency of* $x+1$ *is* $(a+1)2^{s-1}$.

Proof. By Lemma 4.6,

$$(x+1)^{2^s+(a-2)2^{s-1}} = 2^{a-1}b(x)(x+1)^{2^{s-1}} + a(x)$$

for some $b(x)$ is invertible and $a(x)$ s.t. $2^a|a(x)$. So, $a(x)=0$ and

$$(x+1)^{2^s+(a-2)2^{s-1}} = 2^{a-1}b(x)(x+1)^{2^{s-1}}.$$

So,

$$(x+1)^{2^s+(a-2)2^{s-1}}(x+1)^{2^{s-1}-1} = 2^{a-1}b(x)(x+1)^{2^s-1}$$

meaning

$$(x+1)^{2^s+(a-1)2^{s-1}-1} = 2^{a-1}b(x)(x+1)^{2^s-1} \neq 0.$$

Finally,

$$(x+1)^{2^s+(a-1)2^{s-1}} = 2^{a-1}b(x)(x+1)^{2^s} = 0.$$

Hence the nilpotency of $x+1$ is $2^s + (a-1)2^{s-1} = (a+1)2^{s-1}$. □

The two proofs for Lemma 3.8 can be adapted to this setting with the same substitutions as before.

Lemma 4.8. *In* $\frac{GR(2^a,m)[x]}{\langle x^{2^s}-1\rangle}$*, any ideal is at most a-generated.*

As was the case with most of the structure results, the Hamming distance results in Section 3 can easily be adapted to this setting. The main results needed are the Hamming Distances for the codes in $\frac{GR(2,m)[x]}{\langle x^{2^s}-1\rangle}$. These distances again were obtained in [7].

Lemma 4.9 (Corollary 4.12, [7])**.** *In* $\frac{GR(2,m)[x]}{\langle x^{2^s}-1\rangle}$*, for* $0 \leq i \leq p^s$

$$d(\langle (x+1)^i\rangle) = \begin{cases} 1 & \text{if } i = 0,\\ 2 & \text{if } 1 \leq i \leq p^{s-1} \text{ where } 0 \leq \beta \leq p-2,\\ 2^{k+1} & \text{if } 2^s - 2^{s-k} + 1 \leq i \leq p^s - p^{s-k} + 2^{s-k-1},\\ & \text{where } 1 \leq k \leq s-1,\\ 0 & \text{if } i = 2^s, \end{cases}$$

Remark 3. *Given Lemma 4.9, the same method as in Section 3 of Remark 2 can be applied here to compute the Hamming distances for codes in* $\frac{GR(2^a,m)[x]}{\langle x^{2^s}-1\rangle}$.

References

[1] T. Abualrub and R. Oehmke. Cyclic codes of length 2^e over Z_4. *Discrete Appl. Math.*, 128 (1):3–9, 2003. International Workshop on Coding and Cryptography (WCC 2001) (Paris).

[2] T. Abualrub and R. Oehmke. On the generators of $\mathbb{Z}_4$ cyclic codes of length 2^e. *IEEE Trans. Inform. Theory*, 49(9):2126–2133, 2003.

[3] G. Bini and F. Flamini. *Finite commutative rings and their applications*. The Kluwer International Series in Engineering and Computer Science, 680. Kluwer Academic Publishers, Boston, MA, 2002. ISBN 1-4020-7039-X. x+176 pp. With a foreword by Dieter Jungnickel.

[4] A. R. Calderbank and N. J. A. Sloane. Modular and p-adic cyclic codes. *Des. Codes Cryptogr.*, 6(1):21–35, 1995.

[5] G. Castagnoli, J. L. Massey, P. A. Schoeller, and N. von Seemann. On repeated-root cyclic codes. *IEEE Trans. Inform. Theory*, 37(2):337–342, 1991.

[6] H. Q. Dinh. Negacyclic codes of length 2^s over Galois rings. *IEEE Trans. Inform. Theory*, 51(12):4252–4262, 2005.

[7] H. Q. Dinh. On the linear ordering of some classes of negacyclic and cyclic codes and their distance distributions. *Finite Fields Appl.*, 14(1):22–40, 2008.

[8] H. Q. Dinh and S. R. López-Permouth. Cyclic and negacyclic codes over finite chain rings. *IEEE Trans. Inform. Theory*, 50(8):1728–1744, 2004.

[9] S. T. Dougherty and Y. H. Park. On modular cyclic codes. *Finite Fields Appl.*, 13(1):31–57, 2007.

[10] P. Kanwar and S. R. López-Permouth. Cyclic codes over the integers modulo p^m. *Finite Fields Appl.*, 3(4):334–352, 1997.

[11] H. M. Kiah, K. H. Leung, and S. Ling. Cyclic codes over $\mathrm{GR}(p^2, m)$ of length p^k. *Finite Fields Appl.*, 14(3):834–846, 2008.

[12] B. R. McDonald. *Finite rings with identity*. Marcel Dekker Inc., New York, 1974. ix+429 pp. Pure and Applied Mathematics, Vol. 28.

[13] G. H. Norton and A. Sălăgean. On the Hamming distance of linear codes over a finite chain ring. *IEEE Trans. Inform. Theory*, 46(3):1060–1067, 2000.

[14] G. H. Norton and A. Sălăgean. Strong Gröbner bases and cyclic codes over a finite-chain ring. In *International Workshop on Coding and Cryptography (Paris, 2001)*, volume 6 of *Electron. Notes Discrete Math.*, page 11 pp. (electronic). Elsevier, Amsterdam, 2001.

[15] G. H. Norton and A. Salagean. Cyclic codes and minimal strong Gröbner bases over a principal ideal ring. *Finite Fields Appl.*, 9(2):237–249, 2003.

[16] H. Özadam and F. Özbudak. A note on negacyclic and cyclic codes of length p^s over a finite field of characteristic p. *pre-print*.

[17] V. S. Pless and Z. Qian. Cyclic codes and quadratic residue codes over Z_4. *IEEE Trans. Inform. Theory*, 42(5):1594–1600, 1996.

[18] A. Sălăgean. Repeated-root cyclic and negacyclic codes over a finite chain ring. *Discrete Appl. Math.*, 154(2):413–419, 2006.

[19] J. H. van Lint. Repeated-root cyclic codes. *IEEE Trans. Inform. Theory*, 37(2):343–345, 1991.

[20] Z.-X. Wan. Cyclic codes over Galois rings. *Algebra Colloq.*, 6(3):291–304, 1999.

[21] J. Wolfmann. Negacyclic and cyclic codes over Z_4. *IEEE Trans. Inform. Theory*, 45(7):2527–2532, 1999.

Department of Mathematics, Ohio University, Athens, Ohio-45701, USA

Department of Mathematics, Ohio University, Athens, Ohio-45701, USA